IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF Samsung Galaxy J2, IMEI#352475102856901 Serial# R28KC19JAZL TCL A501DL IMEI# 015293006625960 Part# GPALA501CGB seized from the person of RICHARD ZANGARI	Case No. 20-1103-MJ

AFFIDAVIT IN SUPPORT OF APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH TARGET CELLPHONES

I, Ted Wang, being duly sworn under oath and deposed, state the following:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since July 2018. Since January 2019, I have been assigned to the Joint Terrorism Task Force (JTTF) of the Philadelphia Division of the FBI. My duties with the JTTF include investigations of domestic terrorism criminal matters of Title 18 of the United States Code including, but not limited to threatening communication, bomb threats, threats to critical infrastructure, acts of terrorism, fraudulent financial filing and weapons of mass destruction violations. Prior to my employment with the FBI, I was a quality continuous improvement engineer and industrial automation consultant in the pharmaceutical and manufacturing industry of the Fortune 500 and Fortune 1000 companies for approximately 6 years.

2. The information contained in this affidavit is either known to me personally, was relayed to me by other law enforcement officers. This affidavit is intended to show only that there

is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. This affidavit is based upon information I have gained from my investigation, my training and experience, as well as information received from others, including law enforcement officers. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant, and therefore I have not included every fact known to me concerning this investigation.

4. I make this affidavit in support of an application for a search warrant authorizing the examination of a Samsung Galaxy J2 cellular phone, IMEI #352475102856901 and a TCL cellular phone, model A501DL (together the "Target Cellphones"), currently located at the FBI Philadelphia Office, as further described in Attachment A. Both devices belong to RICHARD ZANGARI, and were seized from him when he was arrested on April 28, 2020. The search of the Target Cellphones would be conducted to find evidence of violations of 18 U.S.C. §§ 115(a)(1)(B), Threat to Government Official, 18 U.S.C. §§ 844(e), Use of Communication Facility To Make A Threat and 18 U.S.C. §§ 875(c), Interstate Communication of A Threat to Injure on the devices, as further described in Attachment B.

5. In summary, based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that RICHARD ZANGARI placed numerous threatening phone calls and voicemails at various law enforcement agencies, including but not limited to United States Marshal Service and Pennsylvania State Police . There is also probable cause to believe that evidence of those crimes will be found on the Target Cellphones.

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: a wireless telephone (or mobile phone, or cellular phone) is a handheld wireless devices used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log: which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: a digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage medium to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: a portable media player is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media.

d. GPS: a GPS navigation device uses the Global Positioning System to display its current location. If often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices contain records of the addresses or locations involved in such navigation. The Global Positioning System ("GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate atomic clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combines with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna received signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDS: A Personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as a wireless communication device and are used to access the Internet and send and receive email. PDAs usually include a memory card or other removable store media for storing data and a keyboard and/or touch screen for entering data. Removable storage media includes various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the

same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology.

BACKGROUND ON CELLULAR PHONES, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

7. Cellular phones and more advanced devices known as "smart phones" today function similar to computers and can run computer software and applications, create and edit files, go on the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions.

8. Cellular telephones like the Target Cellphones may also include GPS technology for determining the location of the device and for mapping and navigation features.

9. Based on my knowledge, training, and experience, I know that cellular phones and smart phones, like the Target Cellphones, can store electronic data and information for long periods of time. For instance, things that have been viewed via the Internet on the cellular or smart phone are typically stored for some period of time, and can be recovered by law enforcement with forensic tools. Likewise, GPS information—such directions to a location, or the route an individual traveled—can be stored on the cellular phone for some time, and obtained with forensic tools. Cellular phones and smart phones also may contain SD cards and/or SIM cards, which also store data such as pictures, videos, text messages, contact lists, call logs and other data.

10. Based on my training and experience I know that cellular phones like the Target Cellphones have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that or suggests who possessed or used the device.

11. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the search warrant, but also forensic evidence that establishes how the Target Cellphones were used, the purpose of their use, who used them, when, and where. There is probable cause to believe that this forensic electronic evidence might be on the Target Cellphones because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution: evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with the appropriate familiarity with how an electronic device works, may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can merely be reviewed by a review team and passed along to investigators. Whether data stored on the computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

12. Because this warrant seeks only permission to examine a device already in law enforcement possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

PROBABLE CAUSE

13. The Federal Bureau of Investigation Joint Terrorism Task Force along with other federal, state and local agencies have been investigating a series of threatening voicemails that threatened an un-named US Attorney, Attorney General William Barr, city police officer(s) and the William J Green Jr. Federal Building in Philadelphia PA.

A. ZANGARI Charged Based on April 15, 2020 Voicemail to Federal Defender's and Subsequently Arrested With the Target Cellphones.

14. On or about April 15, 2020, your Affiant received a copy of voicemail ZANGARI left with the Philadelphia Federal Defender's Office. The call was placed via a blocked phone number to the Philadelphia Federal Defender's Office public telephone number, 215-928-1100. During the call ZANGARI spoke about napalm, stating:

> The first person that comes near me, we are gonna go see Jesus together. You know who Jesus is? Here, let me show you, here's the Bible. You know what a Bible is? Ain't nobody got any business coming around me, unless it's for work. That ain't no shit. Understand me? Because I'm not trying to be prejudice against these people.

15. On April 21, 2020, criminal complaint for ZANGARI's arrest was reviewed and warrant signed by Magistrate Judge Jacob Hart.

16. On April 28, 2020, at approximately 9:00 am, ZANGARI walked into the lobby of Williams Green Federal Building at 600 Arch St Philadelphia. He placed items he had with him into two bins as he proceeded through the security screening. Once he went through the security he was arrested transported to Federal Bureau of Prisoner (BOP), where BOP took custody.

17. Of the items ZANGARI placed into the bins, there were two phones, a Samsung Galaxy J2 and a TCL A501DL—the Target Cellphones. When SA Wang called the Target Number, the Samsung Galaxy J2 began to ring. Both devices were then placed on Airplane mode and turned off.

B. Other Threatening Voicemails

i. October 4, 2019 – U.S. Marshals Service Voicemail

18. On October 4, 2019, ZANGARI left a voicemail with Philadelphia division of USMS, where he claimed that he "gave the US Attorney plenty of chances" and "… he [US Attorney] is all out of chances…" and "…he's walking on a thin string…" ZANGARI further mentioned he wanted the US Attorney and the Magistrate Judge to "…sign it, to go straight to the death chamber." However, ZANGARI did not specify what the "it" was.

ii. November 21, 2019 – U.S. Marshals Service Voicemail

19. On October 4, 2019, ZANGARI left a voicemail with Philadelphia division of USMS, ZANGARI talked about "…murdering one of you fucking cops here…" to get the money "they have." He did not specify who "they" were. He later spoke about "…putting a bullet…" into someone, again unspecified, because "…and I want my money. I figure I can do whatever I want here, it's called extortion…"

iii. February 3, 2020 – U.S. Secret Service Voicemail

20. Between the hours of 3:45 am and 4:00 am, male who identified himself as RICHARD ZANGARI left a voicemail at the Philadelphia division of USSS, where he stated Vice President had 24 hours to sign something, but did not mention what would happen if his demands were not filled within the 24 hour time frame.

iv. April 5, 2020 – U.S. Secret Service Voicemail

21. Numerous voicemails were left starting approximately 4:54 pm at the Philadelphia division of USSS using the 267-680-2615 (Target Number). Telephone records show the subscriber for the Target Number is RICHARD ZANGARI. In the voicemails, ZANGARI said, "…I want to know when the fucking idiot U.S. Attorney is fucking singing my … I'm cutting his fucking hand off. You all better be armed tomorrow with AR-15s inside that fucking building. I don't give a fuck."

v. April 5, 2020 – Pennsylvania State Police Voicemail

22. Numerous voicemails were left with PSP using the Target Number. In the voicemails ZANGARI stated:

> US Attorney here and I'm going to cut his fucking hand off, understand I just signed myself here a death penalty. Understand me? I should include William Barr at Washington at the Department of Justice. Understand me? That ain't no fucking shit, I will cut his motherfucking hand off… That U.S. Attorney he's a fucking dead man inside that federal building. Understand me? If he doesn't sign it, Ima cut his fucking hand off. And I guarantee I'm going to get the fuck out of this fucking city alive. Understand me? He's a fucking dead man here period. Understand me? This is what I do, I, (INAUDIBLE), who I want to fucking threat. Nobody tells me what to do here. Understand this is my city.

vi. April 16, 2020 – Federal Defender's Office Voicemail

23. A voicemail was left with the Federal Defender's Office, where ZANGARI stated, "Now get that fucking moron in that building, US Attorney, to sign it or he's fucked for what it is. So I'm going to tell you sign it by fucking tomorrow morning."

CONCLUSION

24. The voicemails collected thus far in the investigation, as described above, demonstrates that there is probable cause to believe that ZANGARI was the caller who repeatedly called the various federal, state and local law enforcement agencies and left threatening voicemails regard un-named US Attorney, un-named federal magistrate judge, Attorney General William Barr and un-specified police officer(s) between October 2019 until now, in violation of 18 U.S.C. §§ 115(a)(1)(B), Threat to Government Official, 18 U.S.C. §§ 844(e), Use of Communication Facility To Make A Threat and 18 U.S.C. §§ 875(c), Interstate Communication of A Threat to Injure. Further, there is probable cause that evidence of the above crimes will be found in the information associated with the Target Number requested to be seized in this search warrant application.

25. Accordingly, a search warrant is requested to perform a forensic digital examination of the Target Cellphones in order to search for additional evidence of the crimes described in this affidavit. For instance, there is probable cause to believe that the Target Cellphones could contain records of ZANGARI placing calls to the various agencies. There is also probable cause to believe that the Target Cellphones could contain GPS information about ZANGARI's during the days and times of the calls. The Target Cellphones are currently in storage in a secure space at the FBI Offices in Philadelphia. In my training and experience, I know that

the Target Cellphones have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when Target Cellphones first came into possession of the FBI.

/s/ Ted Wang
Ted Wang
Special Agent
Federal Bureau of Investigation

Sworn to before me over the telephone and signed by me pursuant to Fed.R.Crim. P. 4.1 and 4(d) on June 29, 2020.

/s/ Richard A. Lloret
HONORABLE RICHARD A. LLORET
U. S. MAGISTRATE JUDGE

ATTACHMENT A
(Property to be Searched)

A Samsung Galaxy J2 cell phone, model SM-J260T1, IMEI 352475102856901. A TCL cell phone, model A501DL, IMEI# 015293006625960, Part# GPALA501CGB. Both devices were seized by the and the FBI from the person of RICHARD ZANGARI on April 28, 2020, incident to ZANGARI's arrest, and currently located at the FBI Philadelphia Division.

ATTACHMENT B (Items to be Searched for and Seized)

1. All records on the devices described in Attachment A that relate to violations of Title 18, United States Code, Section 844(e) (Use of Communication Facility To Make A Threat), Section 115(a)(1)(B), (Threat to Government Official), Section 875(c), (Interstate Communication of A Threat to Injure), between September 4, 2019 and April 28, 2020, including:

a. Documents in electronic form, including correspondence, records, opened or unopened emails, text messages, voicemail messages, call logs, chat logs, internet history, social media application data, GPS data and map history, mobile payment application data, address book and calendar entries, photographs, and videos, relating to the calls placed to the various law enforcement agencies, where threats were left.

2. Evidence of user attribution showing who used or owned the device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history, even if the evidence was created/stored on the phone prior to September 4, 2019. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including, but not limited to the following:

a. Forms of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

b. Data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system, including any and all electronic data which can be collected, analyzed, created, displayed, converted, stored, concealed, or transmitted, or similar computer impulses or data.

c. Stored electronic information and communications, including but not limited to: telephone or address directory entries consisting of names, addresses and telephone numbers; logs of telephone numbers dialed, telephone numbers of missed calls, and telephone numbers of incoming calls; schedule entries; stored memoranda; stored text messages; stored photographs; stored audio; and stored video.

3. Evidence and contents of logs and files on the device, such as those generated by the device's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, opened, saved, or deleted.